IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: John BORDER *et al.*	Confirmation No.: 1446
Application No.: 09/662,072	Examiner: El Chanti, Hussein
Filed: September 14, 2000	Group Art Unit: 2457
Attorney Docket No.: PD-200053	

For: PERFORMANCE ENHANCING PROXY AND METHOD FOR ENHANCING PERFORMANCE

REPLY BRIEF

Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Reply Brief is submitted in response to the Examiner's Answer mailed June 9, 2009.

I. STATUS OF THE CLAIMS

Claims 3, 5-9, 11-29, 32, 34-38, and 40-59 are pending and are on appeal. Claims 1, 2, 4, 10, 30, 31, 33, 39, and 60 have earlier been canceled.

Claims 3, 5-9, 11-29, 32, 34-38, and 40-59 remain rejected under 35 U.S.C. §102 (e) as anticipated by *Yates et al*. (US 6,167,438).

II. GROUNDS OF REJECTION TO BE REVIEWED

Whether claims 3, 5-9, 11-29, 32, 34-38, and 40-59 are anticipated under 35 U.S.C. §102 (e) based on *Yates et al*. (US 6,167,438)?

III. ARGUMENT

Appellants maintain and incorporate the positions presented in the Appeal Brief filed April 2, 2009, but present further refutation of certain assertions presented in the Examiner's Answer.

In response to Appellants' argument that *Yates et al.* fails to disclose a multiplexing element configured to selectively multiplex the spoofed connections onto a single connection of the second type, the Examiner refers to col. 8, line 55-col. 9, line 59 of *Yates et al.* and argues that a connection is made between a client and a server through a router where the router has a snooper application capable of spoofing client requests and establishing connections to servers to obtain requested content. In particular, the Examiner argues that the router establishing the connection between the client and the cache server has a snooper that identifies whether a packet received from a client is a {SYN} packet or a {GET} packet. If the packet is a {SYN} packet, then the snooper spoofs the server connection until a {GET} packet is received, referring to col. 9, line 54-col. 10, line 3 of *Yates et al.* When a {GET} message is received, the router combines the {SYN} and {GET} messages into a single {SYN+GET} message and the message is sent on a separate connection to a cache server to service the request, referring to col. 10, line 16-col. 11, line 55.

Thus, the Examiner concludes that *Yates et al.* teaches the snooper ("spoofing element"), which intercepts connections that have {SYN} messages (messages of a first type) and that the router is a multiplexing element that combines the {SYN} and {GET} messages onto a single connection with a single {SYN+GET} request (single connection of the second type). Accordingly, the Examiner is interpreting the connection between the client and the router in *Yates et al.* as the claimed "first type of connection" and the connection established between the

router and the cache server as the claimed "second type of connection" used to transmit a combined {SYN+GET} request to the cache server.

The flaw in the Examiner's reasoning is that the Examiner is equating types of messages, e.g., {SYN} and {GET} with types of **connections**, as claimed. In claim 3, for example, the proxy communicates with the other network entities "via a first type of connection and a second type of connection, wherein the proxy establishes multiple connections of the first type associated with different applications." The transmission or receipt of a {SYN} or {GET} message is **not** a communication "**via a first type of connection** and a second type of connection." Similarly, the mere sending of a plurality of {SYN} messages is **not** the same as the establishment of "**multiple connections of the first type associated with different applications**." As an example, when two parties are engaged in a telephone conversation over a telephone line, a connection must first be established between the telephone sets and then messages, e.g., conversation, may be relayed over that connection, but the conversation itself is **not** the connection. Thus, it is a perverse and tortured, as well as a flawed, interpretation for the Examiner to insist that messages sent over a connection are equivalent to the connections themselves.

Since messages are not connections, the Examiner's interpretation that the router is a multiplexing element that combines the {SYN} and {GET} messages onto a single connection with a single {SYN+GET} request (single connection of the second type) is also flawed. The instant claims recite "a multiplexing element configured to selectively multiplex the spoofed **connections** onto a **single connection of the second type**"(claim 3) or something similar. Since {SYN} and {GET} messages are not connections, and are only messages that are sent over the **same** connection, the combining of {SYN} and {GET} messages is not a multiplexing of spoofed connections onto a single connection of the second type, as claimed. Whereas the instant

disclosure reveals two different types of connections, e.g., a TCP connection and a backbone connection shown in Fig. 3 and described at page 6, lines 13-15, of the specification, the connection over which the {SYN} and {GET} messages in *Yates et al.* are sent (see Fig. 3 of *Yates et al.*, for example) is the same. Thus, there is only one type of connection, e.g., the connection between client and home server depicted in Fig. 3, in *Yates et al.* Therefore, *Yates et al.* does not disclose the claimed "first type of connection" and "second type of connection" and cannot anticipate the instant claims under 35 U.S.C. §102 (e).

Even considering the Examiner's interpretation of the "first type of connection" to be the connection between the router and the client in *Yates et al.* and the "second type of connection" to be the connection between the router and the cache server, these may be connections, but they are not different **types** of connections (e.g., TCP connection, backbone connection), as claimed. Moreover, while there may be connections between the router and the client and between the router and the cache server in *Yates et al.*, these are not "spoofed connections" which may be **selectively multiplexed** "onto a single connection of the second type," as claimed. The actual connection between the client and the router ("first type") is not "spoofed," as required by the claims. Further, even if it could be considered to be a spoofed connection, there is no evidence in *Yates et al.* that these connections between the client and the routers are then **selectively multiplexed onto a single connection** between the router and the cache server ("second type").

Accordingly, again, *Yates et al.* cannot anticipate the instant claims under 35 U.S.C. §102 (e).

At page 10 of the Answer, responsive to Appellants argument that *Yates et al.* does not define a spoofing rule in a spoofing profile or a prioritizing rule in a prioritizing profile, the Examiner contends that since the connection between the client and the router in *Yates et al.* is a

"first type of connection," where the snooper on the router receives {GET} messages and spoofs the connection, *Yates et al.* does teach "spoofing connections of the first type."

As explained above, *Yates et al.* does not disclose the use of different "types" of connections. But, to the extent that one may call the single type of connection in *Yates et al.* "a connection of the first type, it is not the connection that is spoofed in *Yates et al.* but, rather, it is the home server that is spoofed (see, e.g., col. 9, lines 66-67). Thus, there is no "spoofing element only spoofing connections of the first type associated with at least one of applications…" in *Yates et al.*

The Examiner further argues, at page 10 of the Answer, that *Yates et al.* teaches routing {GET} messages in accordance with neighborhood information "set of rules" in a current routing tree "spoofing profile" and that responsive to a determination of the neighborhood information in a tree, the snooper selects a cache server to forward the requested messages, referring to col. 13, lines 17-50, of *Yates et al.*

The Examiner's rationale is in error. The routing of messages in accordance with some set of rules (rules which are not clearly discloses by *Yates et al.*) is not a disclosure of a "spoofing element" that "defines the at least one spoofing rule in a spoofing profile" or of a "prioritizing element" that "defines the at least one prioritizing rule in a prioritizing profile" as recited in claims 7 and 13, for example, respectively. Moreover, the Examiner has previously defined the router of *Yates et al.* as the claimed spoofing element and the router is not disclosed as defining a "spoofing rule in a spoofing profile" or a "prioritizing rule in a prioritizing profile." In any event, what is spoofed in *Yates et al.* is the home server 20, as recited, e.g., at col. 9, lines 66-67. Neither the router nor the home server in *Yates et al.* comprises a "spoofing element" that "defines the at least one spoofing rule in a spoofing profile" or a "prioritizing element" that

"defines the at least one prioritizing rule in a prioritizing profile." No such "spoofing profile" or "prioritizing profile" is disclosed or suggested by *Yates et al*. Examples of such a "spoofing profile" or "prioritizing profile" are given at page 12, lines 16-30, and page 16, line 15-page 17, line 23, respectively, of the instant specification. Thus, in accordance with the instant disclosure, certain criteria, e.g., destination IP address, source IP address, TCP port numbers, TCP options, and IP differentiated services field, may be specified by a user in producing a selective TCP spoofing rule. The set of rules selected by the user is defined in a selective spoofing selection profile. Similarly, certain criteria, e.g., destination IP address, source IP address, IP next protocol, TCP port numbers, UDP port numbers, and IP differentiated services, may be specified by a user as a set of rules in a prioritization profile. The determination by a resource manager at a cache server of which routing trees certain information is on and of any downstream cache servers on each tree, as described in *Yates et al*., at col. 13, lines 23 *et seq.* does not disclose or suggest a "spoofing element" that "defines the at least one spoofing rule in a spoofing profile" or a "prioritizing element" that "defines the at least one prioritizing rule in a prioritizing profile" in any manner, let alone as those terms are employed and defined in the instant application. Therefore, dependent claims 7, 13, 36, and 42 are patentable separately from their independent claims and the Honorable Board is respectfully urged to reverse the rejection of these claims under 35 U.S.C. §102 (e) even if the Honorable Board sustains the rejection of the independent claims.

IV. CONCLUSION AND PRAYER FOR RELIEF

The claims require, *inter alia*, a multiplexing element configured to selectively multiplex the spoofed connections onto a single connection of the second type, and a "spoofing element" that "defines the at least one spoofing rule in a spoofing profile" or a "prioritizing element" that "defines the at least one prioritizing rule in a prioritizing profile," but *Yates et al.* fails to disclose any of these features. Appellants, therefore, request the Honorable Board to reverse the Examiner's rejection of claims 3, 5-9, 11-29, 32, 34-38, and 40-59 under 35 U.S.C. §102 (e).

To the extent necessary, a petition for an extension of time under 37 C.F.R. §1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 504213 and please credit any excess fees to such deposit account.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

July 21, 2009
Date

/Phouphanomketh Ditthavong/
Phouphanomketh Ditthavong
Attorney for Applicant(s)
Reg. No. 44658

Errol A. Krass
Attorney for Applicant(s)
Reg. No. 60090

918 Prince Street
Alexandria, VA 22314
Tel. (703) 519-9952
Fax (703) 519-9958